RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: SBV-M05

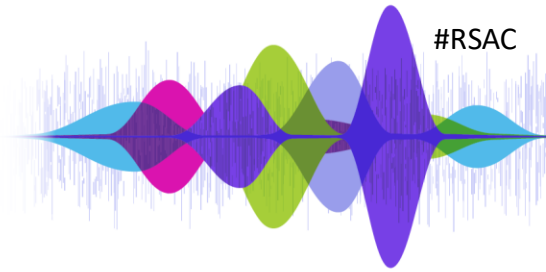
Saasified Crime: AiTM on the Rise

Rik van Duijn

Hacker
Attic Security
https://www.linkedin.com/in/rik-van-duijn/

Wesley Neelen

Hacker
Attic Security
https://www.linkedin.com/in/wesleyneelen/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Who are we

- Wesley Neelen
  - Ethical hacker
  - OSCP / OSEP / ..
  - 10+ years of experience
- Rik van Duijn
  - Ethical hacker
  - OSCP / OSCE
  - 10+ years of experience

Our goal

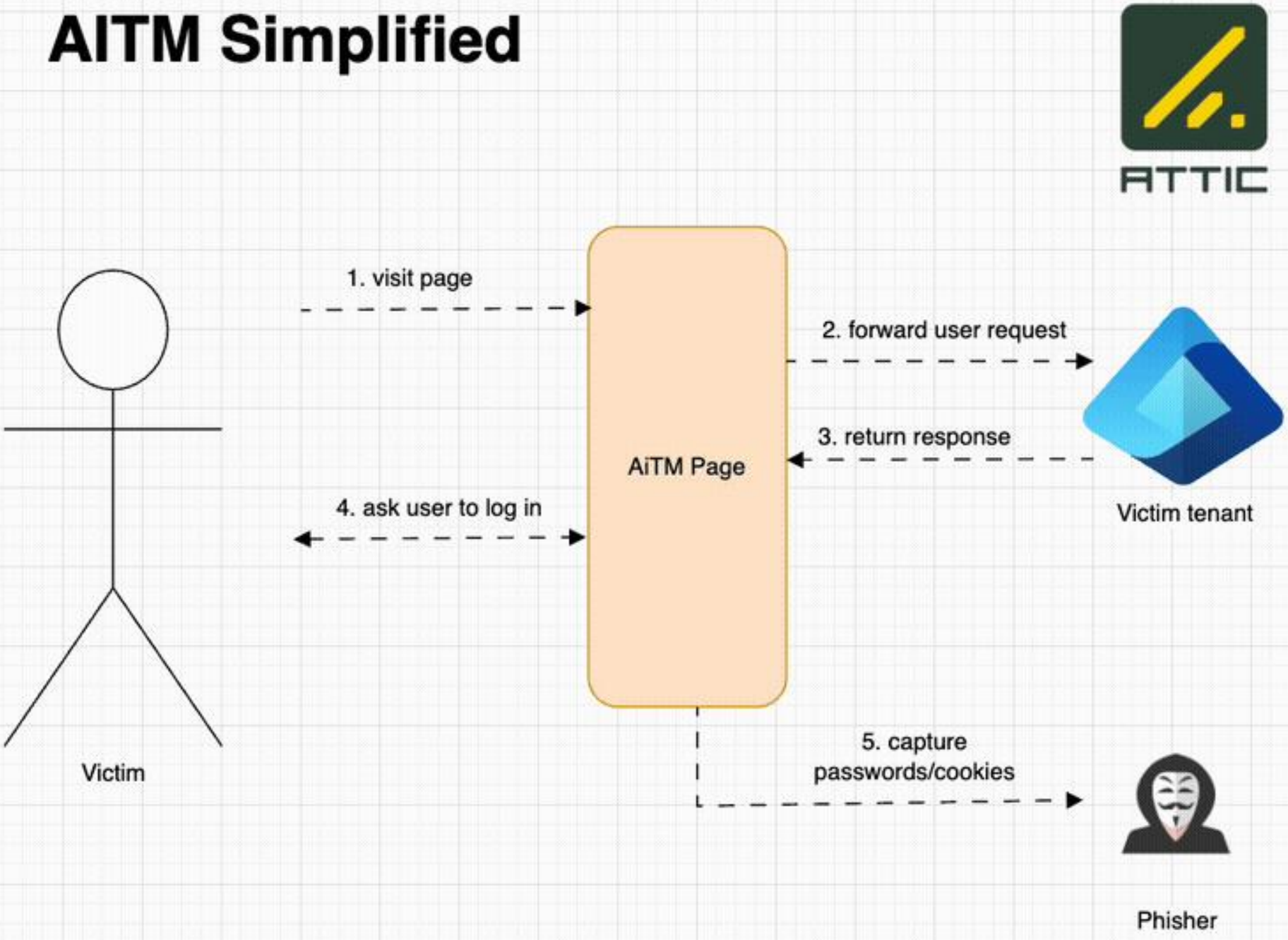
- Improve IT-security for the largest group of companies possible. No nation-state ironclad enterprise grade security but a small improvement each and every day.

atticsecurity.com

The problem

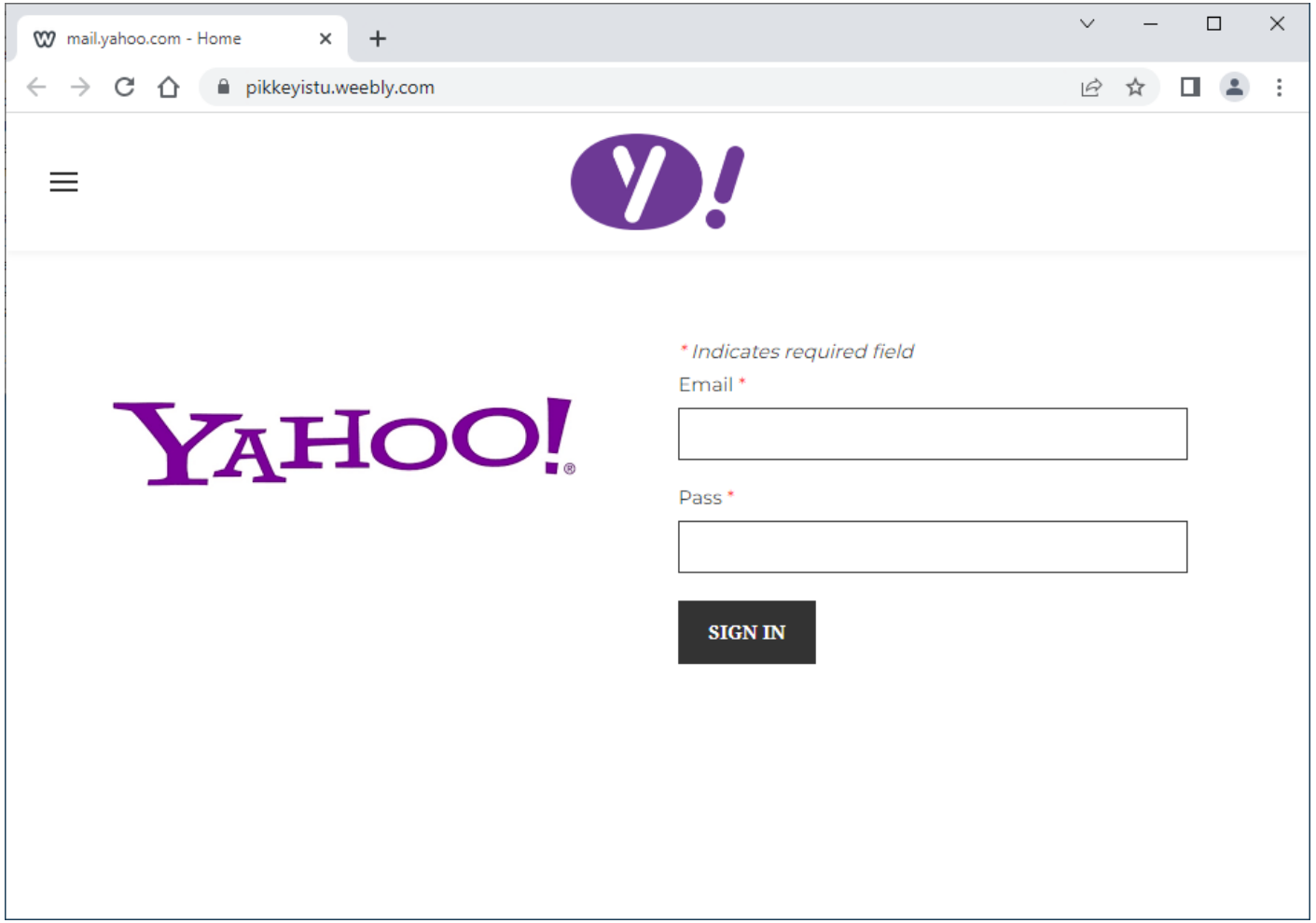
Theres been an increase in phishing attempts that incorporate MFA.

AITM Simplified

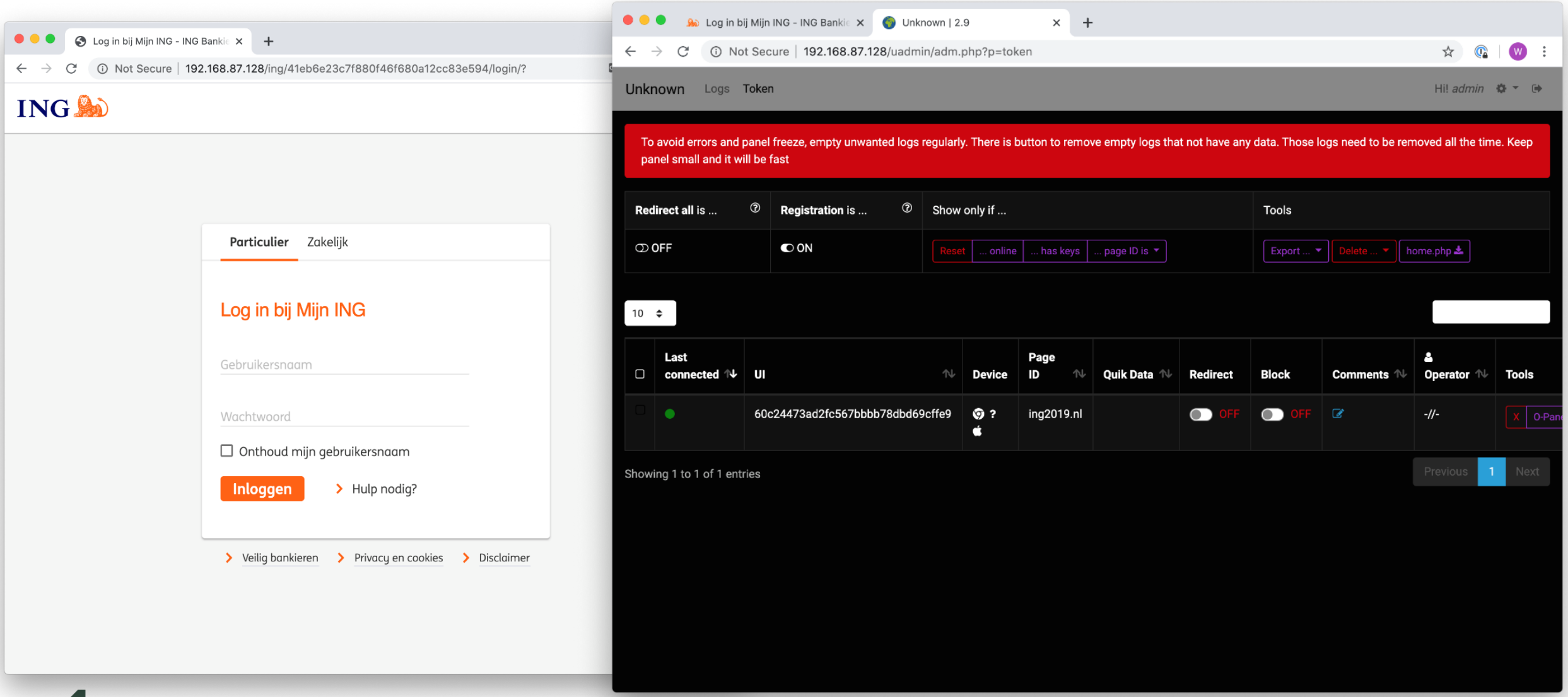


Some history

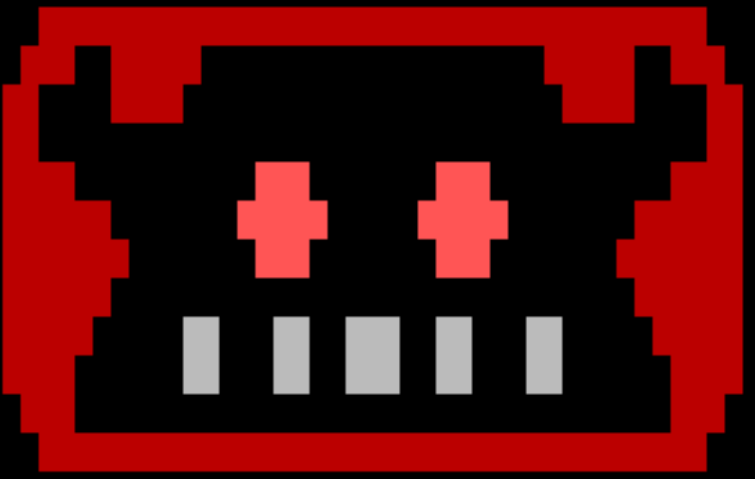
Phishing used to be possible at scale



Some history



```
root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/
```



```
 ____________   _ _   _ _____ _____ _____ _____ _____
|  ___| ___ \ | | | | |  __ \|_   _|  __ \|  _  /  ___|
| |__ | |_/ / | | | | | |  \/  | | | |  \/| | | \ `--.
|  __||    /  | | | | | | __   | | | | __ | | | |`--. \
| |___| |\ \  \ \_/ / | |_\ \ _| |_| |_\ \\ \_/ /\__/ /
\____/\_| \_|  \___/   \____/ \___/ \____/ \___/\____/
```

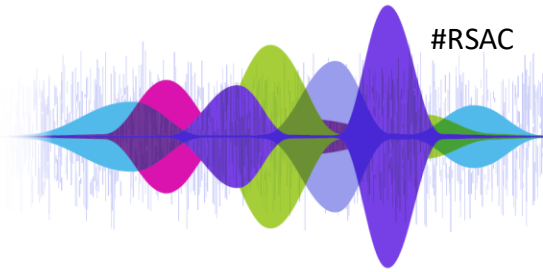
no nginx - pure evil

by Kuba Gretzky (@mrgretzky) version 2.0.0

```
[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [^_^] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilgin
ost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359
([redacted])
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions

+-----+-----------+----------+----------+--------+-----------------+---------------------+
| id  | phishlet  | username | password | tokens |    remote ip    |        time         |
+-----+-----------+----------+----------+--------+-----------------+---------------------+
| 19  | google    |          |          | none   | [redacted]      | 2018-05-28 08:23    |
+-----+-----------+----------+----------+--------+-----------------+---------------------+

[08:24:22] [^_^] [0] Username: [[redacted]@gmail.com]
[08:24:29] [^_^] [0] Password: [[redacted]]
[08:24:41] [^_^] [0] all authorization tokens intercepted!
[08:24:41] [imp] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com
: sessions

+-----+-----------+-------------------------+---------------+----------+----------------+-----------------+
```

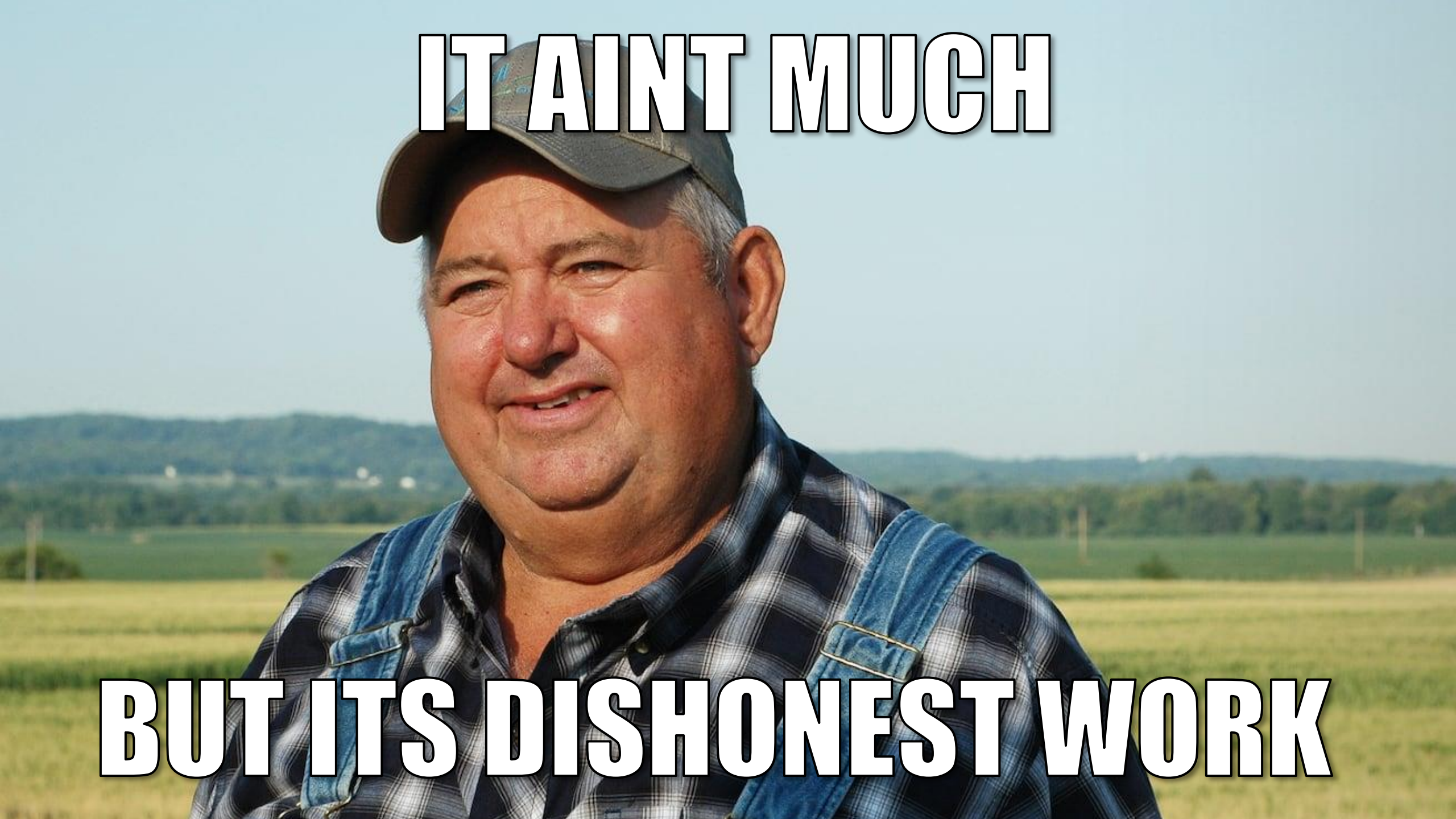
RSAC™ 2025 Conference

Why now?



WHY NOW?

1. SaaS
2. More and more mfa, jay ☺
3. It works (at scale)


IT AINT MUCH
BUT ITS DISHONEST WORK

WHY NOW?

NEWS 29 AUG 2023

Microsoft Warns of Adversary-in-the-Middle Phishing Platforms

FORBES > INNOVATION > CYBERSECURITY

New Gmail & M365 Warning As 2FA Security Bypass Hack Confirmed

Davey Winder Senior Contributor

Davey Winder is a veteran cybersecurity writer, hacker and analyst.

Follow

A new phishing kit is targeting Gmail and Microsoft email accounts — and it can even bypass 2FA

News By Sead Fadilpašić published March 26, 2024

Two-factor authentication isn't what it used to be

When you purchase through links on our site, we may earn an affiliate commission. Here's how it works.

Microsoft Threat Intelligence
@MsftSecIntel

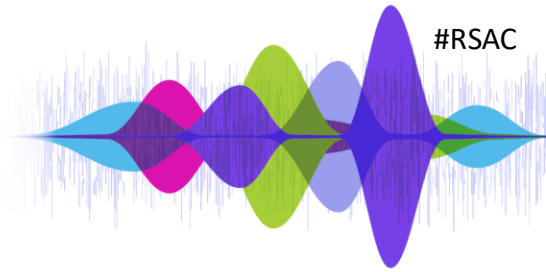
Microsoft has detected a 111% year-over-year increase in token replay attacks, and incidents are continuing to grow. msft.it/6011lSgZ7

Team Email Scam: What You Need

ıail

Published: April 26, 202

WHY NOW?



	URL		Age
1	**URL:** 365docusend.digitalarchiving.it.com/nUTkM/ **IP:** 172.67.150.70 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 200	32 minutes **Via:** manual
2	**URL:** finalclosingdisclosures.whisperingvoids.it.com/3Y30Y/ **Redirect from:** finalclosingdisclosures.whisperingvoids.it.com/3Y30Y#testemail%40outlook.com **IP:** 172.67.191.142 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US) **Tags:** falconsandbox	Public 200	47 minutes **Via:** api
3	**URL:** amphenolindustrialoperations.docvaulthost.com/qRT5a/ **IP:** 2606:4700:3032::6815:3c5f - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 200	4 hours **Via:** manual
4	**URL:** documentations-informations-files.jkarnerica.com/DreR3/ **IP:** 188.114.96.3 - **Server:** cloudflare **GeoIP:** NL - AS13335 (CLOUDFLARENET, US)	Public 200	7 hours **Via:** manual
5	**URL:** schwaitzerendustries.obscurepath.eu/Exw2W/ **Redirect from:** ad.planbplus.co.kr/web_ref/?ref=https%3A%2F%2Fschwaitzerendustries.obscurepath.... **IP:** 172.67.160.16 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 200	7 hours **Via:** manual
6	**URL:** schwaitzerendustries.obscurepath.eu/Exw2W/ **IP:** 172.67.160.16 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 200	7 hours **Via:** manual
7	**URL:** fdhdfv.sombrasusurhanrante.it.com/Ooy1h/ **IP:** 104.21.96.1 - **Server:** cloudflare	Public 200	9 hours **Via:** manual
8	**URL:** onlineverifynowonlineservicsesupdates2899787jhd6.auth-airdr0preward.es/k7JyE/ **IP:** 188.114.97.3 - **Server:** cloudflare **GeoIP:** NL - AS13335 (CLOUDFLARENET, US)	Public 200	9 hours **Via:** manual
9	**URL:** rutlandplastics.silenciyifodorado.it.com/Qy2Pw/ **Redirect from:** atlantique-ts.be/redirect.php?v=85af91d75204b73 **IP:** 2606:4700:3036::6815:1d7 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 200	9 hours **Via:** api

URL		Age
URL: olx-pl.lolaskiv.sbs/cdn-cgi/phish-bypass?atok=NUSmgxnOuU1VOr2WYgeEFUMPKXmHR4Uce... **IP:** 172.67.170.102 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 403	21 minutes **Via:** manual
URL: butanse.shop/cdn-cgi/phish-bypass?atok=B8uJLSG7Ketk730cAOe5fVbH5X0Pm50vuMUmLgv6... **Redirect from:** butanse.shop/ **IP:** 188.114.97.3 - **Server:** cloudflare **GeoIP:** NL - AS13335 (CLOUDFLARENET, US)	Public 403	51 minutes **Via:** manual
URL: wwess44685.top/cdn-cgi/phish-bypass?atok=I6FJKWSDLTLhWny5W8nqchIIjYAzfw5DAIZ4xX... **Redirect from:** wwess44685.top/ **IP:** 172.67.205.64 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 403	1 hour **Via:** api
URL: www.lululemon-mexico.com./cdn-cgi/phish-bypass?atok=Wip_HhunZbWtNRMq40TZfpK4aOU... **Redirect from:** www.lululemon-mexico.com./ **IP:** 104.21.16.1 - **Server:** cloudflare	Public 403	2 hours **Via:** manual
URL: wwess99876.top/cdn-cgi/phish-bypass?atok=sqM9Ru7FEoT7vRVuooOYKNzmLMf2NplONpqXeD... **Redirect from:** wwess99876.top/ **IP:** 188.114.97.3 - **Server:** cloudflare **GeoIP:** NL - AS13335 (CLOUDFLARENET, US)	Public 403	2 hours **Via:** api
URL: butanse.shop/cdn-cgi/phish-bypass?atok=0fQ522bJeFFYcejCEqHZ7EfDcHF3g2dp6o.IweSC... **Redirect from:** butanse.shop/ **IP:** 188.114.97.3 - **Server:** cloudflare **GeoIP:** NL - AS13335 (CLOUDFLARENET, US)	Public 403	2 hours **Via:** manual
URL: tokionlineodeme.com.tr/cdn-cgi/phish-bypass?atok=ivEaEAO9wm.GPNrtq8SIDyVIVB783W... **Redirect from:** tokionlineodeme.com.tr/ **IP:** 172.67.216.74 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 403	2 hours **Via:** api
URL: konto-dkb.com/cdn-cgi/phish-bypass?atok=27XD63gX8eWPeBnUQK7Mp.VcGb9Iv_zVNERQidP... **Redirect from:** konto-dkb.com/ **IP:** 2606:4700:3035::6815:1079 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 403	4 hours **Via:** automatic **Src:** phishtank
URL: weixe.ir/cdn-cgi/phish-bypass?atok=zYWOSSlhbw5CN.lgNzzx7zSgzZZC9egxuKH.52fDyeg-... **Redirect from:** weixe.ir/txt/rhLWwI4GaRtMLe7.exe **IP:** 172.67.133.70 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 403	4 hours **Via:** api

Booking.com

BBC

Home News Sport Business Innovation Culture Travel Earth Video Live

Booking.com warns of up to 900% increase in travel scams

20 June 2024

Share

Tom Gerken
Technology reporter

The New York Times

TRIPPED UP

Help! My London Rer Apartment Vanished a Out $3,100.

Following instructions she thought came fro woman wired payment for her planned eigh

Booking.com scams that look 'so real' have surged, costing Australians thousands of dollars

By Tom Williams | Scams and Fraud

Tue 30 Jan

NOS Nieuws • Maandag 22 december 2014, 18:19

10.000 klanten Booking.com sla phishing

Booking.com

	URL		Age
1	**URL:** www.verifbooking.com/ **IP:** 162.213.251.110 - **PTR:** server273-5.web-hosting.com - **Server:** LiteSpeed **GeoIP:** US - AS22612 (NAMECHEAP-NET, US)	Public 200	9 hours **Via:** automatic **Src:** certstream...
2	**URL:** com-confirms.live/favicon.ico **IP:** 172.67.154.100 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 200	7 days **Via:** api
3	**URL:** pre-approved.booking-listings-531752.com/images/booking.ico **IP:** 172.67.133.175 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 200	9 days **Via:** api
4	**URL:** booking.com-confirms.live/Oldiskord **IP:** 172.67.154.100 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 403	10 days **Via:** api
5	**URL:** rprtgustrfdroms.world/win/ **Redirect from:** rprtgustrfdroms.world/ **IP:** 188.114.96.3 - **Server:** cloudflare **GeoIP:** NL - AS13335 (CLOUDFLARENET, US)	Public 200	10 days **Via:** api
6	**URL:** pre-approved.booking-listings-531752.com/en/hotel/magnificent-apartment-milano/... **Redirect from:** tinyurl.com/jt88r8er **IP:** 172.67.133.175 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 200	10 days **Via:** manual
7	**URL:** pre-approved.booking-listings-531752.com/en/hotel/magnificent-apartment-milano/... **IP:** 2606:4700:3035::6815:5b1 - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 200	11 days **Via:** manual
8	**URL:** pre-approved.booking-listings-531752.com/en/hotel/magnificent-apartment-copenha... **IP:** 2606:4700:3032::ac43:85af - **Server:** cloudflare **GeoIP:** US - AS13335 (CLOUDFLARENET, US)	Public 200	12 days **Via:** api

Search for domains, IPs, filenames, hashes, ASNs

hash:5522523714d946a5810383bbca991c678457eed981b987d65f352c9fed2dc7d9 | Search | ✖ | Help

Search results (100 / 974, sorted by date, took 168ms)

Showing All Hits | Details: Hidden

URL		Age		Size		IPs		
booking.issue499.com/sign-in?op_token=NxldXFnUr8L11MAp1FDbpv5BP4i6YlfdxFaeE9WKA...	Public	3 days		124 KB	16	3	3	NL
complaint.issue499.com/sign-in?op_token=BibgFny5XF6cO93Rg6B1wAkbmnn1o53T2sn0Mxf...	Public	4 days		116 KB	12	3	3	NL
booking.issue499.com/sign-in?op_token=XIJyoyCQImPLo4AHWO5QqAILZ90TXfr1S9b38H6fu...	Public	7 days		124 KB	16	3	3	NL
booking.issue499.com/sign-in?op_token=NYYSwTQvqDCeLtbfuCGHat6yuPRllLJCI88aXJRjP...	Public	7 days		120 KB	12	3	3	NL
booking.issue499.com/sign-in?op_token=BJts4at4GK9yOuYgUkkxaIakagh7jaLscOWoilhIZ...	Public	7 days		120 KB	12	3	3	NL
booking.issue499.com/sign-in?op_token=zVQ1xkiUDSK0SNzenQcG40dd4GD91hy6tTy8222Ld...	Public	8 days		120 KB	12	3	3	NL
booking.issue499.com/sign-in?op_token=6OpYILE1eHY42I7yOe13c0ufsizgHXT3Cchgg0DI7...	Public	8 days		120 KB	12	3	3	NL
booking.issue104.eu/sign-in?op_token=ACPUBYtOGdEaIMNuAq6IsCRhwMAl5qgJQLsLYRhsNu...	Public	8 days		120 KB	12	3	3	NL
booking.issue104.eu/sign-in?op_token=ao8uVWQJIrScERiDOMAY2IMPvUSeDZ3RsJUtinkgo8...	Public	9 days		120 KB	12	4	3	US
booking.issue499.com/sign-in?op_token=ssDvnM0WDpcqOcOwXD2G1klpDTKjAH8CzIv37HpQf...	Public	10 days		116 KB	12	3	3	NL
complaint.issue499.com/sign-in?op_token=lzT5zryPZ3F4rDO9jsaskBmMSU2gI9C7b2LTj2g...	Public	10 days		116 KB	12	3	3	NL
complaint.issue1473.eu/sign-in?op_token=nlVj4IVozfQRoEYQsNEPXEZjm3xT8IsKyBtkOwb...	Public	12 days		116 KB	12	3	3	NL
complaint.issue412.eu/sign-in?op_token=mMVp6HDbqaQt4E0G1mfxUAqXk8o241V6zHoeXFB7...	Public	12 days		116 KB	12	3	1	US
complaint.issue899.eu/sign-in?op_token=JbFUf1AAwyBPmwWZnQpT4bzIcUVGW6np0TMZABoi...	Public	13 days		116 KB	12	3	1	US
complaint.issue899.eu/sign-in?op_token=V24IzjHM8nDG88bLyKbpZxeWpHUBhj2M4dcIIgLR...	Public	13 days		116 KB	12	3	2	
complaint.room543435.com/sign-in?op_token=i1BkV2q2UGxCi9tl0XcccerDeOPQ33r9hlygI...	Public	14 days		116 KB	12	3	3	NL
complaint.room543435.com/sign-in?op_token=vXHy5jb152b6vrljHtqXcs7pzPzC8FOKLYhI6...	Public	14 days		116 KB	12	3	3	NL
booking.issue257.eu/sign-in?op_token=toU56hH1046wCQ8ACZdNlLh8BWBeRjtZ2pI7fhDVLo...	Public	15 days		116 KB	12	3	3	NL
booking.issue257.eu/sign-in?op_token=0F6O02I1Z85UPLuecAFbNISLG4QDUb3oPYQ0UUrmZg...	Public	15 days		116 KB	12	3	3	NL
complaint.issue01.eu/sign-in?op_token=20MPdF57FIFnuzicBAfl8mEZZy0xmTgRZx6DPhZJr...	Public	15 days		124 KB	16	3	2	US

ATTIC your digital security assistant

Booking.com

Hello Remmelzwaal Erik👋

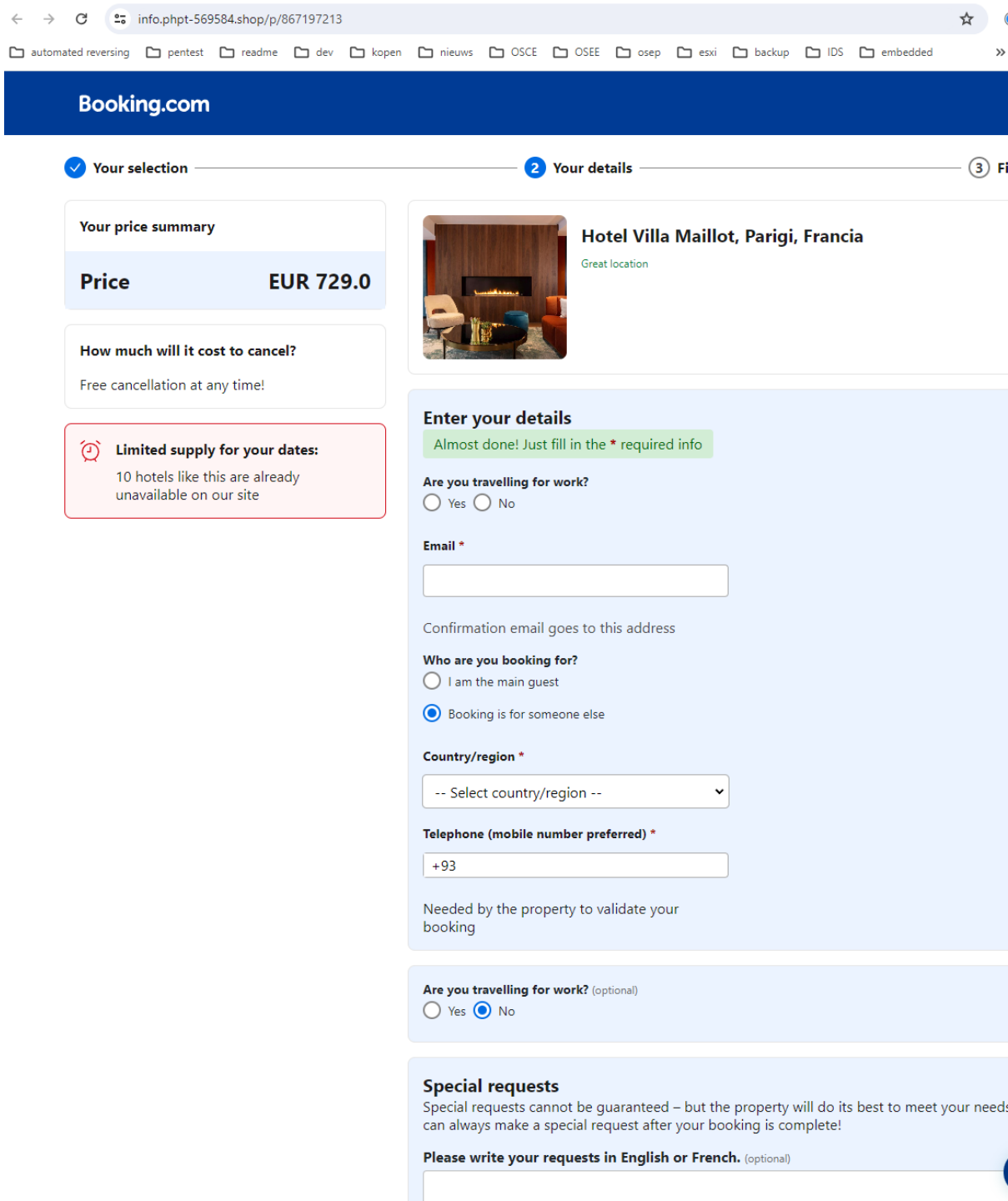
I am your check-in manager Carlos, "Hotel Villa Maillot". I have contacted you via booking.com about the important verification process, but you have not yet completed it.

We have sent you the verification link and instructions via booking.com chat and email.
Please complete the process as soon as possible.

If you didn't see the link in the booking chat, here it is: https://info.phpt-569584.shop/p/867197213

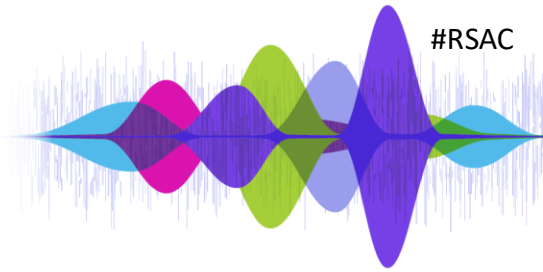
If you have any questions, chat me here and I'll do my best to help you. Thank you for your cooperation and understanding!

14:15



RSAC™ 2025 Conference

ACTORS



Actors

- Storm-1575 (Rockstar2fa/Dadsec/Phoenix)
- Storm-1167 (Flowerstorm)
- EvilProxy
- Mamba2fa
- Tycoon
- Raccoon
- … and more

- Change is coming, more and more non-saas but old-school panel providers are popping up.

Actors - Evilproxy

- Whole dockerized setup
- Might be leaking his real name
- Most tech savvy implementation

07/02/2022

Reverse proxy
Our phishing pages are 100% identical

You get LOGIN, PASSWORD, COOKIES and more info about user

We can help you increase your resistance to phishing attacks. Phishing as a Service (PhaaS) is a security awareness program for everyone in an org
Our phishing simulations are supported by a proprietary software platform. In particular, our backend application offers a complete set of features r
Get a demo completely free for 1 day!
New users without an account in the system - minimum deposit $250

We can help you improve your resilience against phishing attacks. Phishing as a Service (PhaaS) is a security awareness program for all employees
Our phishing simulations are supported by an in-house developed software platform. In particular, our backend application offers the full set of func
Get a demo completely free 1 day!
New users without an account in the system - minimum deposit 250$

+ Services:
- microsoft 10/20/31 days = 150$/250$/400$ (Hotmail, CORP, Remote SSO, ADFS) (auto cookies refresh with internal tool)
- google 10/20/31 days = 250$/400$/600$
- icloud.com 10/20/31 days = 150$/250$/400$ (auto token/cookies refresh up to 2 days with internal tool)
- dropbox.com 10/20/31 days = 150$/250$/400$ (also sign in with google)
- github.com 10/20/31 days = 150 $ /250 $ /400$
- facebook.com 10 /20/31 days = 150 $ /250 $ /400$
- yahoo.com 10/20/31 days = 150 $ /250 $ /400$
- aol.com 10/20/31 days = 150 $ /250 $ / 400$
- twitter 10/20/31 days = 150 $ /250 $ /400$
- wordpress.com 10/20/31 days = 150 $ /250 $ /400$
- pypi.org 10/20/30 days = 150 $ /250 $ /400$
- npmjs.com 10/20/30 days = 150 $ /250 $ /400$
- rubygems.org 10/20/30 days = 150 $ /250 $ /400$

ATTIC
your digital security assistant

Actors - Raccoon

Initially looked like it took over Tycoon but just another actor.

AiTM page management done via email

Based on cloudflare (workers?)

Has a stealers and mailer in the offer

RaccoonO365💥 2FA/MFA🔒 Бог печенья owner

📣 Announcement: Upcoming Price Changes for RaccoonO365 Suite

Dear RaccoonO365 Hat Teams,

We are excited to announce updates to our RaccoonO365 Suite subscription plans, effective somewhere in February, alongside the launch of our new panel. Until then, all services will remain at their current pricing, so take advantage of the existing rates while they last.

Key Updates:

Business Days Only: Plans now count business days (excluding Saturdays and Sundays), allowing you to use your links over weekends at no extra cost.

Updated Subscription Plans (Effective Somewhere in February):

Starter Plan: $250 (12 Business Days, includes Botminator)
🔥 Perfect for short-term projects.

Professional Plan: $320 (25 Business Days, includes Botminator)
🔥 Ideal for quick access and mid-sized projects.

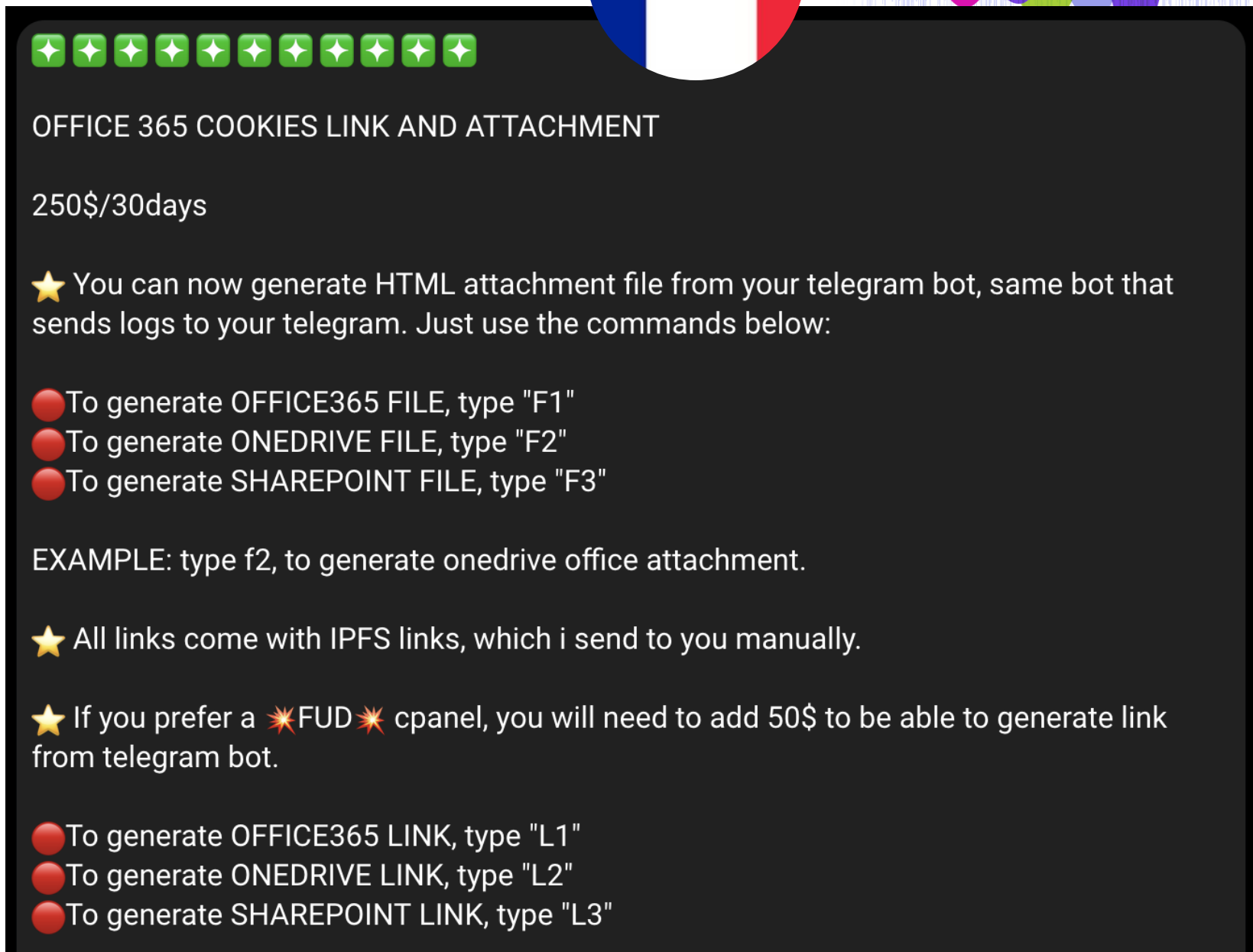
Advanced Plan: $350 (35 Business Days, includes Botminator)
🔥 Great for consistent access needs.

Actors – Mamba2fa

All aitm management done via tg bot

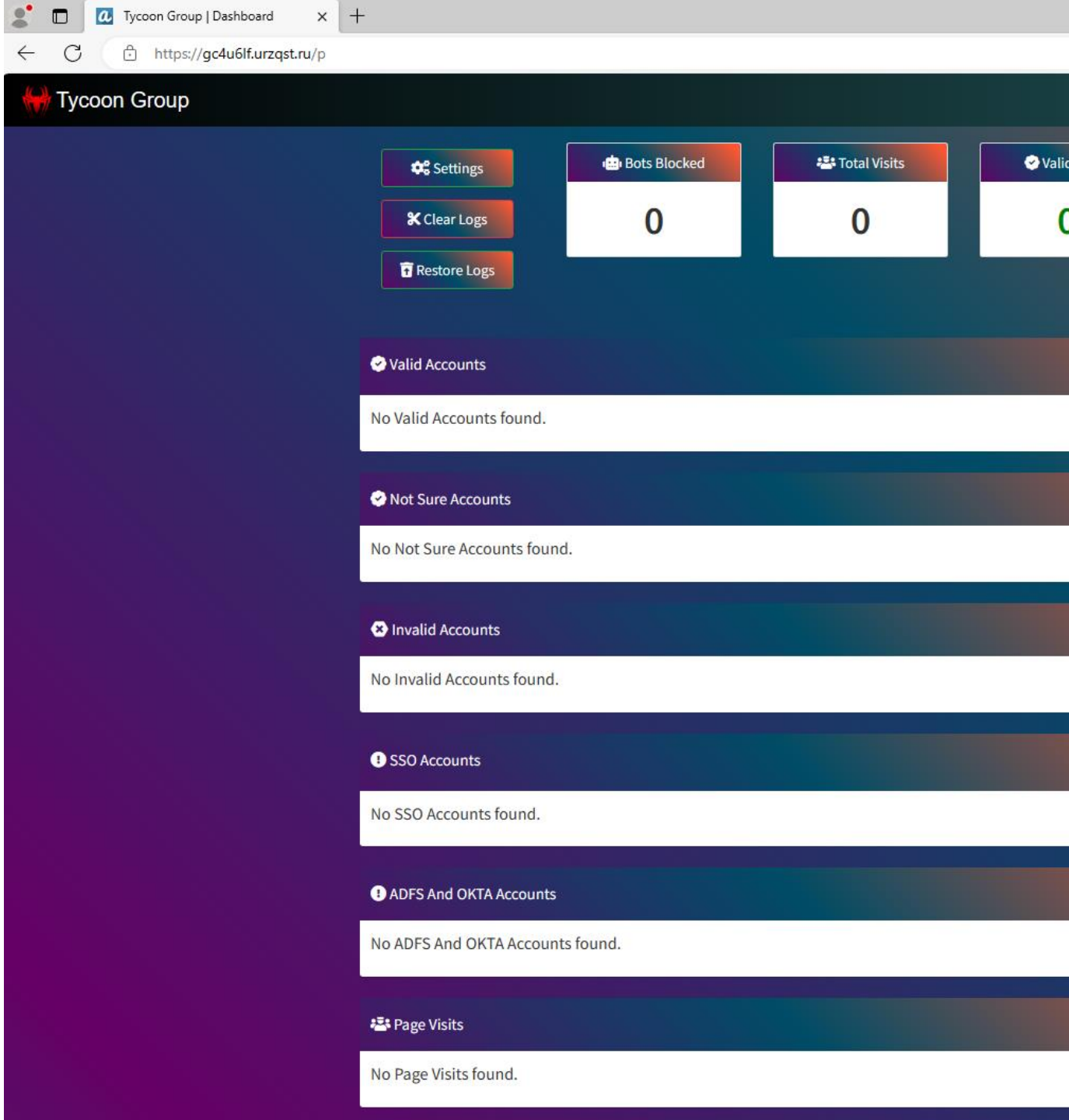
Upsell for more features

Mailer in the offering


OFFICE 365 COOKIES LINK AND ATTACHMENT
250$/30days
⭐ You can now generate HTML attachment file from your telegram bot, same bot that sends logs to your telegram. Just use the commands below:
🔴To generate OFFICE365 FILE, type "F1"
🔴To generate ONEDRIVE FILE, type "F2"
🔴To generate SHAREPOINT FILE, type "F3"
EXAMPLE: type f2, to generate onedrive office attachment.
⭐ All links come with IPFS links, which i send to you manually.
⭐ If you prefer a 💥FUD💥 cpanel, you will need to add 50$ to be able to generate link from telegram bot.
🔴To generate OFFICE365 LINK, type "L1"
🔴To generate ONEDRIVE LINK, type "L2"
🔴To generate SHAREPOINT LINK, type "L3"

Actors - Tycoon

- Is “gone” no public outreach
- New panel looks different, no mention of tycoon.
- Wallets are the same
- Money still comming in.



ATTIC
your digital security assistant

Actors - Tycoon

- 1GvdAwPyTRKmRzybyrfHtbYWVJbecCbTNj
- 19NReVFKJsYYCCFLq1uNKYrUqQE2bB4Jwx
- TMuvWvkX6EYNGqPcSZ7M3HRF8RkHaMm7rq
- 3HF8mTpCDLWDXNVQQhpg49gnEybWwcGGwB

Total Received
5.55831141 BTC
$535,234

Total Sent
5.55831141 BTC
$535,234

Transactions
1,869

Total Received
4.00603784 BTC
$390,514

Total Sent
4.00603784 BTC
$390,514

Transactions
2,219

- 1.2M (dependent on BTC price 😂)

Total Received	270,235.933276 USDT
Total Sent	269,485.933276 USDT
Transactions	1350

Transactions(1350) Total 1000 First < 1 2 3 4 5 > Last

Transaction	Block Height	Age	From	To
6f9683d3238ae49bcf583e...	69606378	38 hours ago	Bybit Hot Wallet (TU4v)	TMuvWvkX6EYNGqPcSZ7...
7a009e5199d867d7ca0ca...	69603847	40 hours ago	TWqPaQSuzdeEnEAiPz8T...	TMuvWvkX6EYNGqPcSZ7...
bbbf259951de8f38381fc6...	69602488	41 hours ago	TJbDBjsgiEG8uTBb4MmZ...	TMuvWvkX6EYNGqPcSZ7...

Anti Robot checks

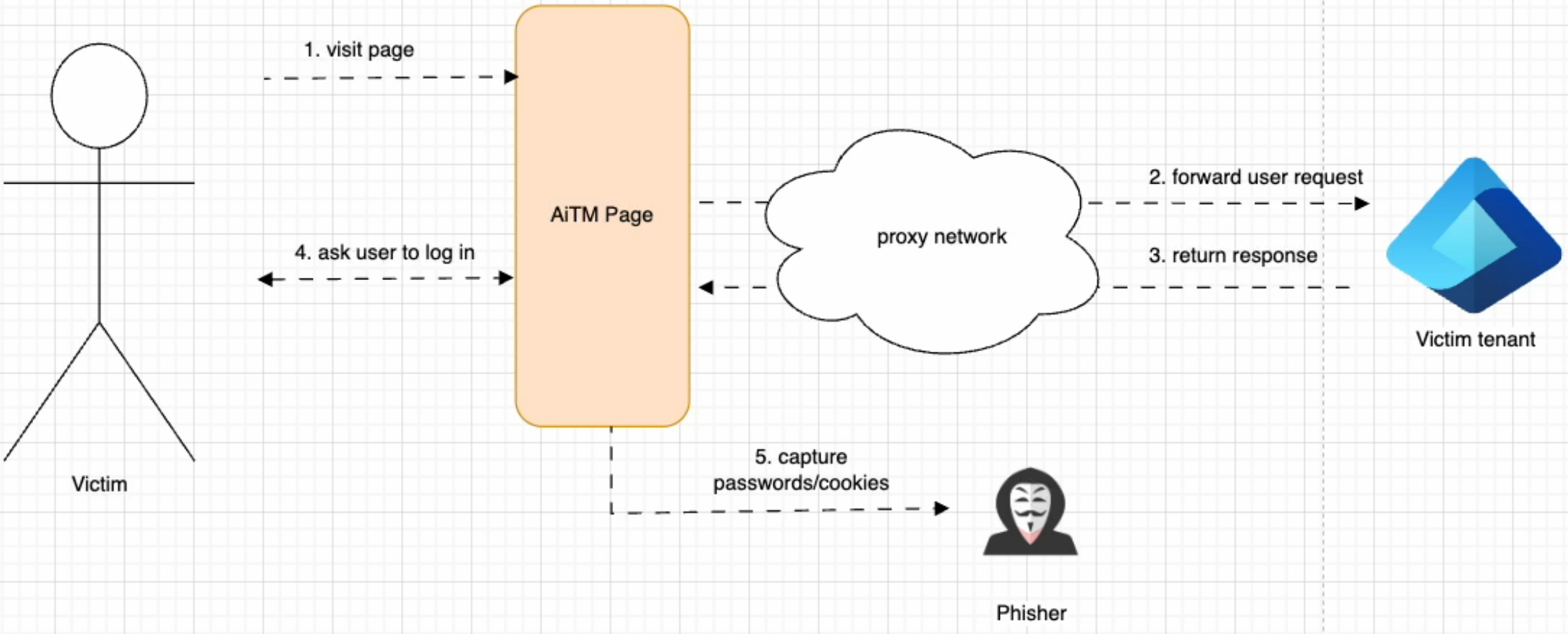
- When you see this, its almost always a problem

Interesting detections

Proxied sign ins

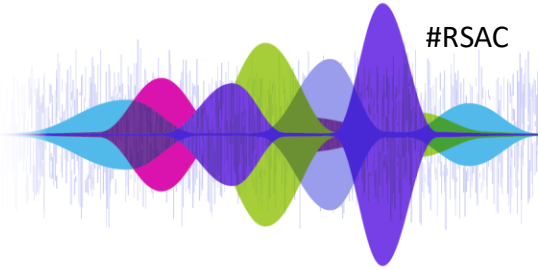
Hides sign ins using:

- VPS systems
- Hacked home pc's



RSAC™ 2025 Conference

PREVENTION AND DETECTION



Prevention for M365 is easy

- … Compared to other SaaS platforms
- For companies with budget

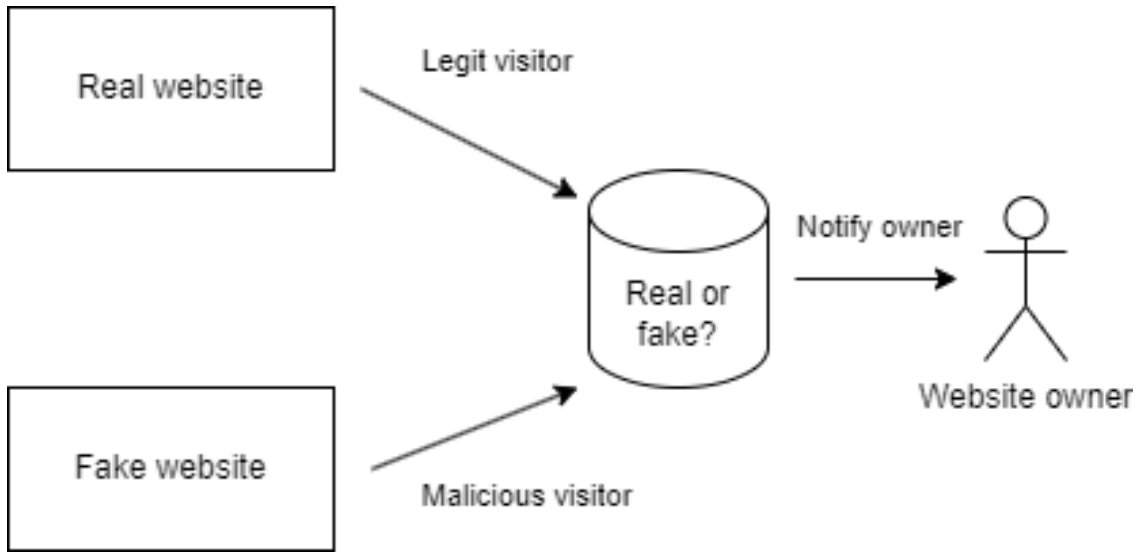
Options:

- Enforce phishing resistant MFA (requires AAD P1/P2)
- Enforce device compliance (requires AAD P1/P2)

Detection

Built detection technique for regular phishing sites (didsomeoneclone.me):

- Inserting a pixel into the real website -> loaded via the real or fake website?



Detection

Pixel + M365?

- Erik: what about Microsoft Custom Branding CSS setting?

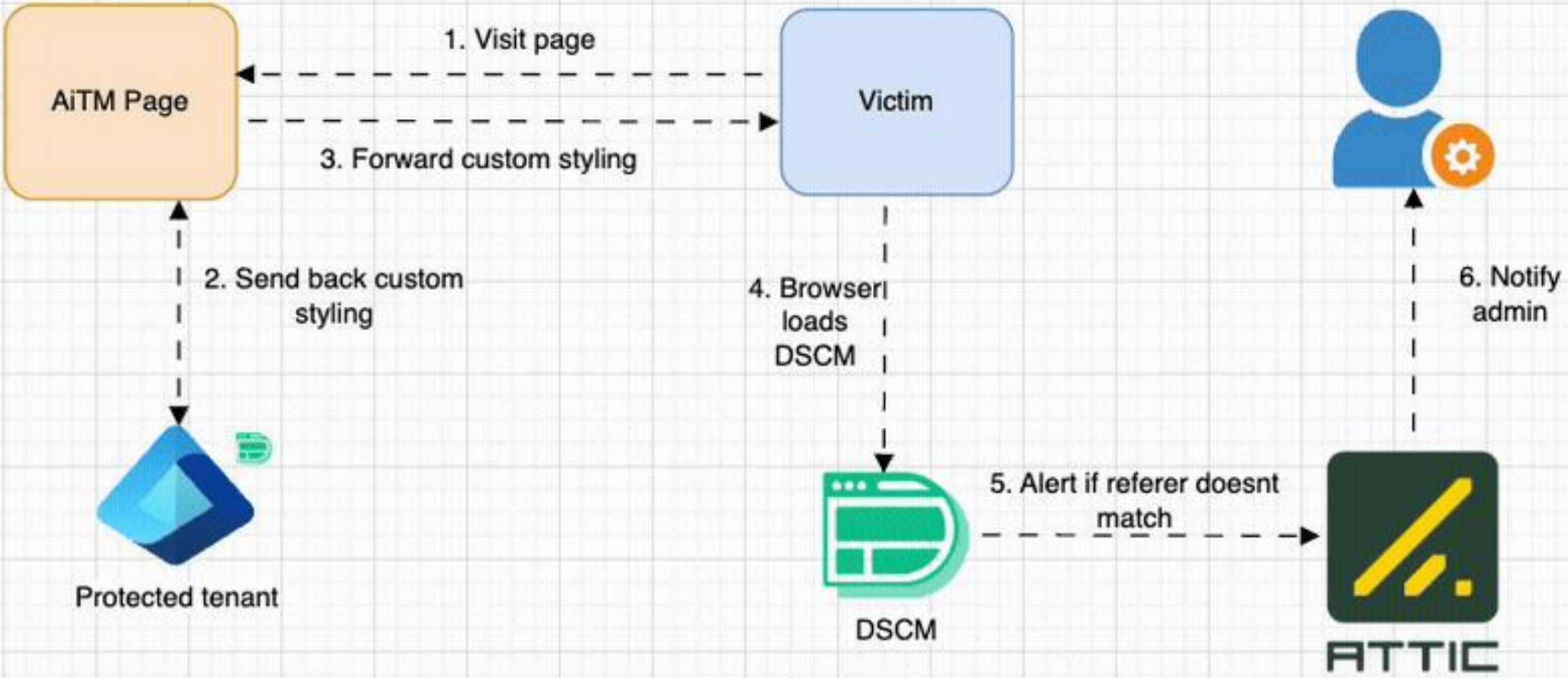
Detection

It works!

Azure Function Tuesday 7:02 PM

Phishing site found [dscm-callbackbec5b5]
Original: microsoftonline.com
Fake: https://login.aitm.tech/

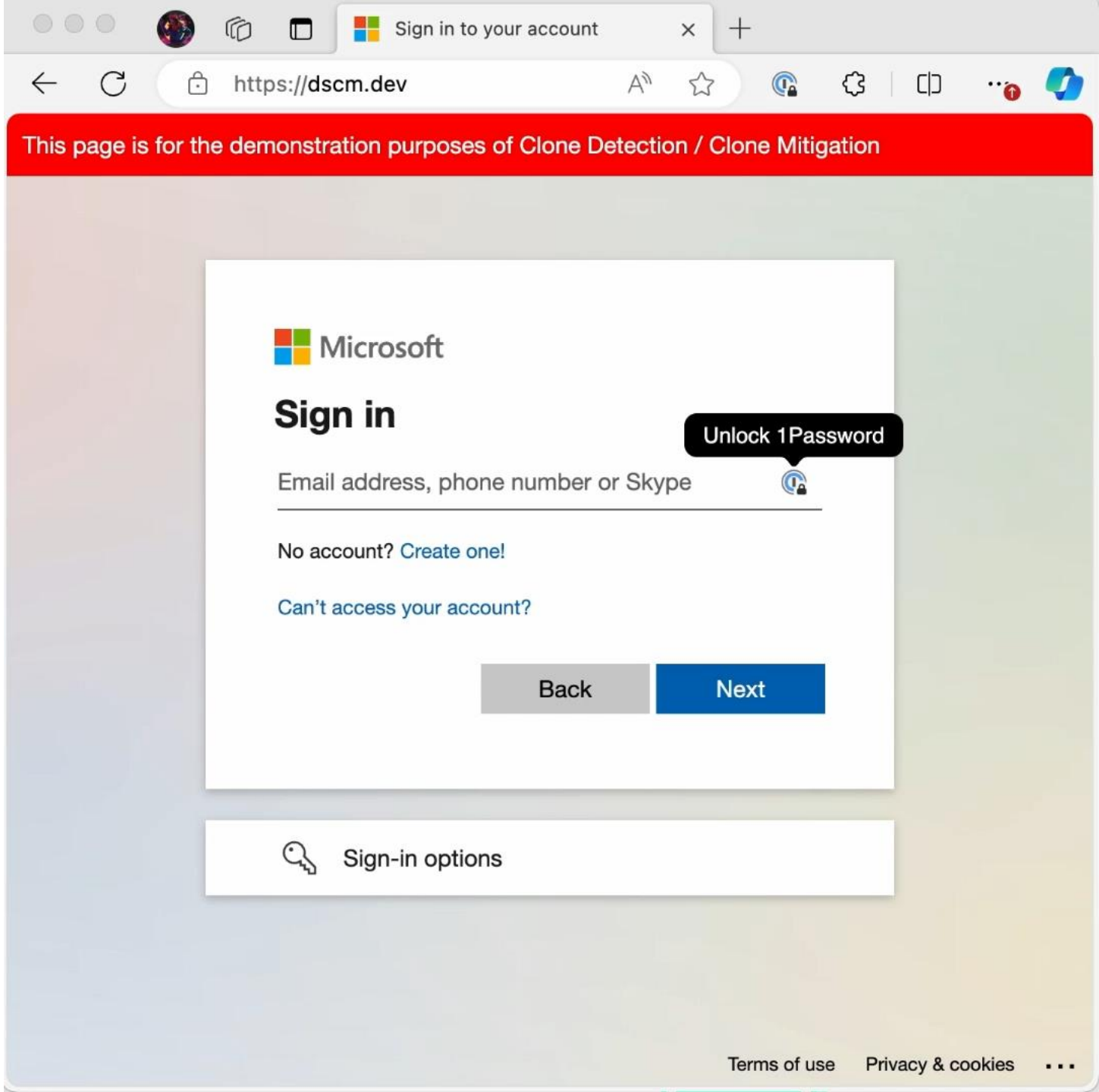
Valid || Not valid


AiTM Page
1. Visit page
Victim
3. Forward custom styling
2. Send back custom styling
4. Browser loads DSCM
6. Notify admin
Protected tenant
DSCM
5. Alert if referer doesnt match
ATTIC

Detection

Pixel + M365?

- Can we mitigate the phishing attack using CSS?

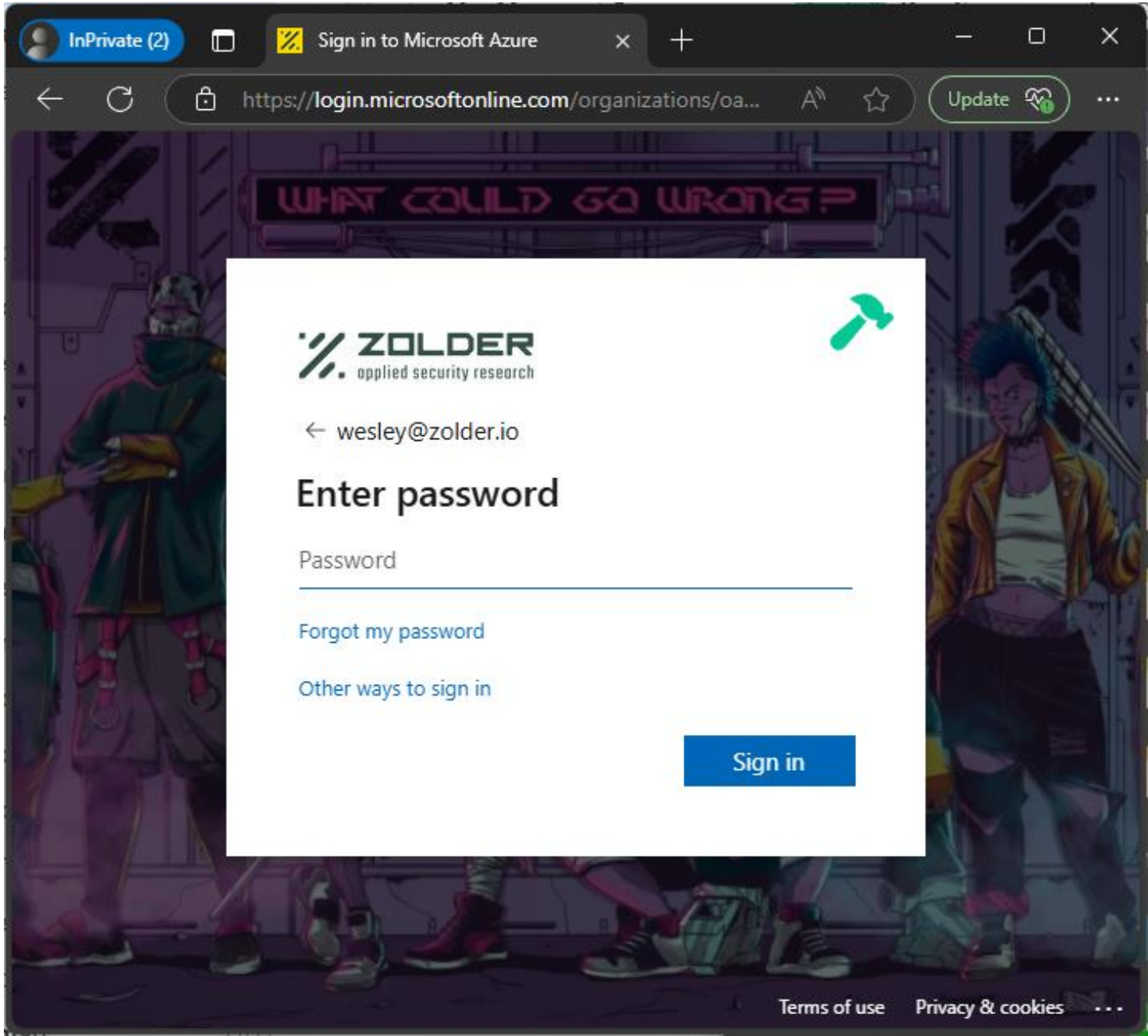


ATTIC
your digital security assistant

Detection

Pixel + M365?

- Showing a verified screen

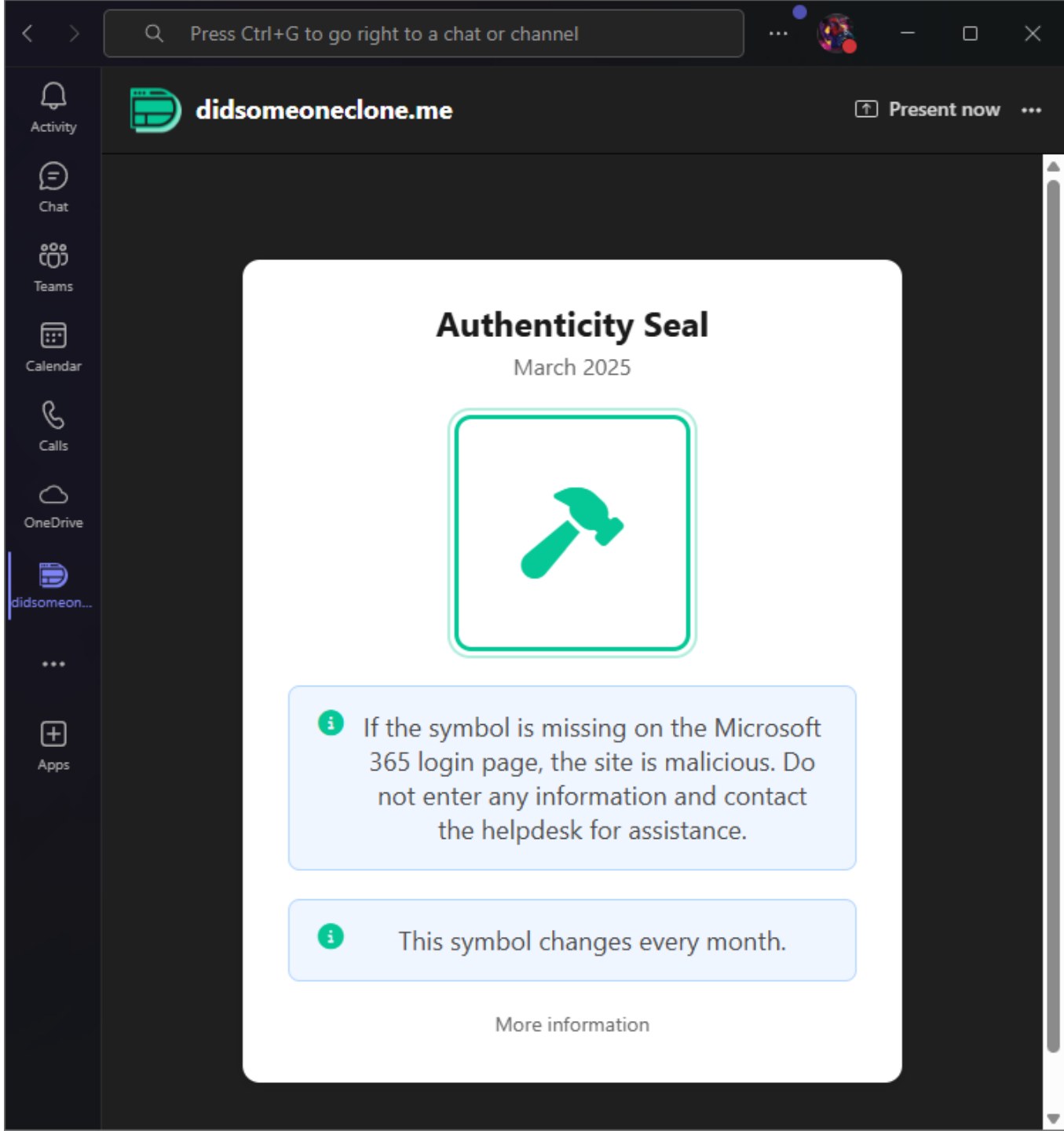


ATTIC
your digital security assistant

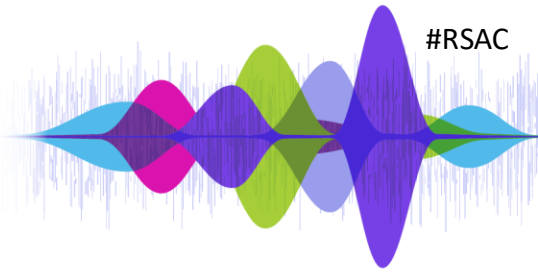
Detection

Pixel + M365?

- Showing a verified screen



ATTIC
your digital security assistant



Detection

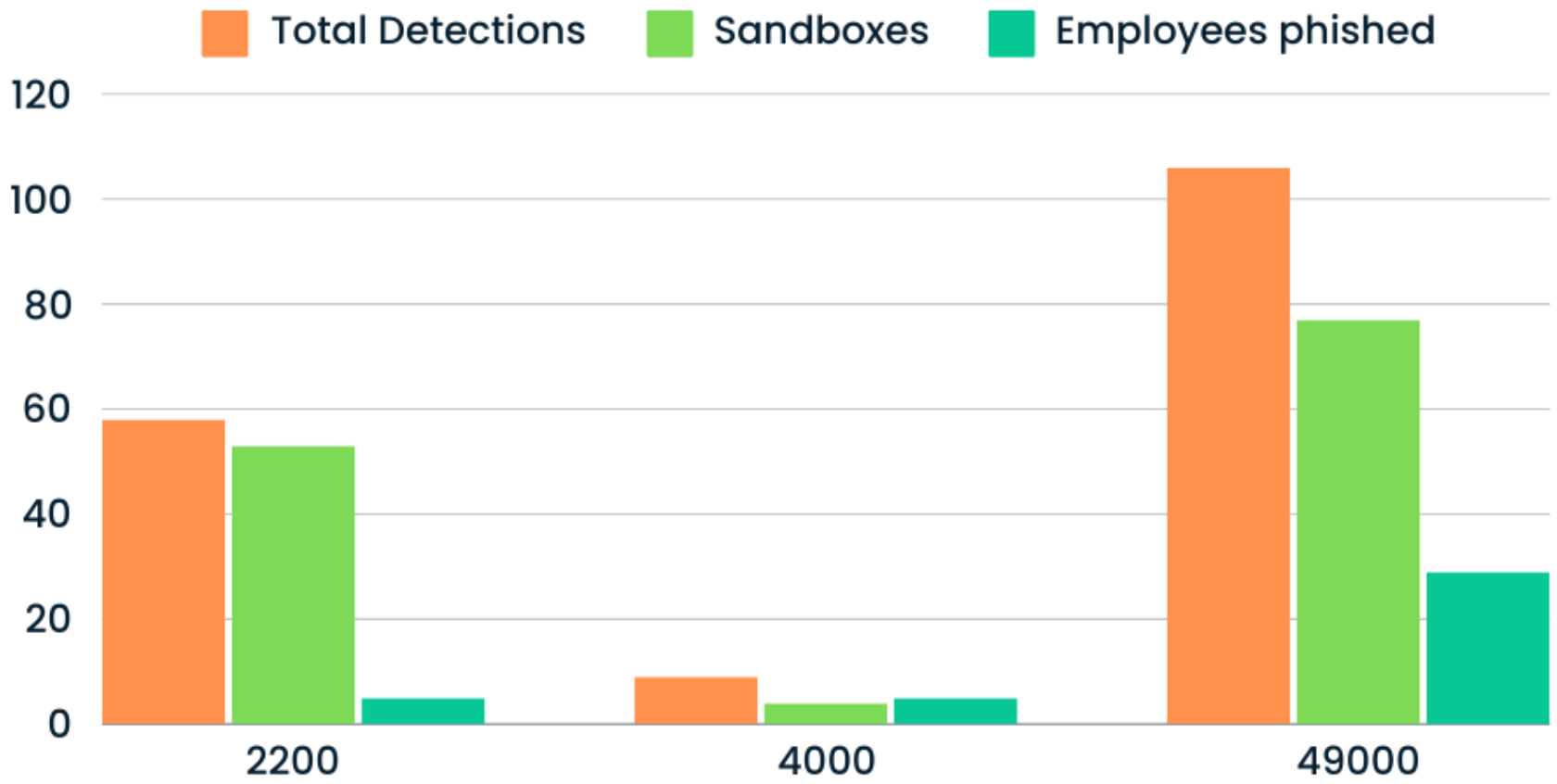
Expecting little detections..

- Reality:
  - **First month**
  - **100** tenants
  - **162** detections

  - **15 months**
  - **483** tenants
  - **2308** detections

Detection

Expecting little detections..



Detection

AITM allows for scale once more

Timestamp ↑	AITM	AutomatedNotification	ClientIP	ClonedDomain
2024-04-09T12:30:04.24...	true	true		https://bnymellons.org/
2024-04-09T14:00:45.97...	true	true		https://bnymellons.org/
2024-04-09T14:30:32.74...	true	true		https://bnymellons.org/
2024-04-09T19:30:18.00...	true	true		https://bnymellons.org/
2024-04-15T21:09:11.25...	true	true		https://bnymellons.org/
2024-04-20T08:00:05.93...	true	true		https://bnymellons.org/

2024-09-03T14:30:01.40...	IN_PROGRESS	true		https://commandsmedic...	commandsmedical.com
2024-08-30T17:16:00.89...	IN_PROGRESS	true		https://commandsmedic...	commandsmedical.com
2024-09-04T00:18:55.04...	IN_PROGRESS	true		https://commandsmedic...	commandsmedical.com
2024-08-30T19:11:16.19...	IN_PROGRESS	true		https://commandsmedic...	commandsmedical.com
2024-09-03T12:42:01.07...	IN_PROGRESS	true		https://commandsmedic...	commandsmedical.com
2024-09-03T11:28:15.25...	IN_PROGRESS	true		https://commandsmedic...	commandsmedical.com
2024-09-03T17:59:30.02...	IN_PROGRESS	true		https://commandsmedic...	commandsmedical.com

ATTIC your digital security assistant

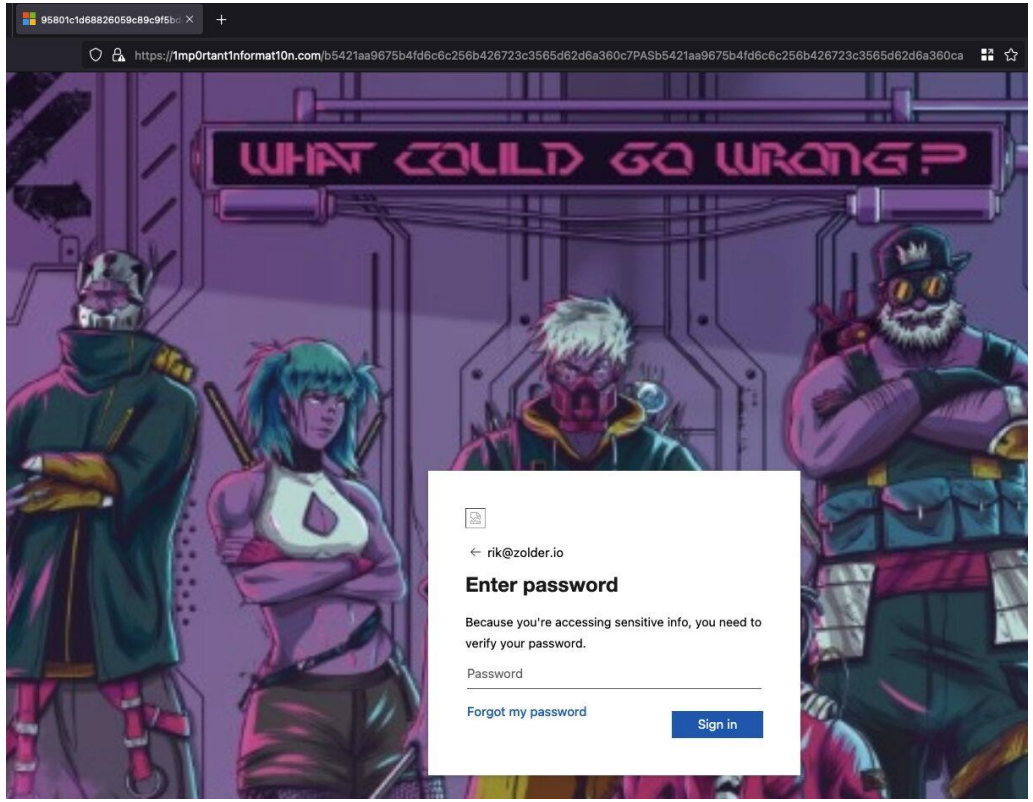
Detection

False positives?

- Limited, some examples:
  - login.microsoft.com
  - tasks.office.com
  - autologon.microsoftazuread-sso.com
  - login.windows.net

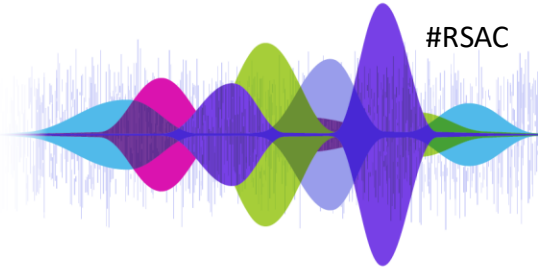
Very reliable detection, after fine-tuning

Interesting detections



200	GET	1mp0rtant1nformat10n....	api-as1f?email=rik@zolder.io&data=logo	axios.min.js:1 (xhr)	html	763 B
200	GET	1mp0rtant1nformat10n....	api-as1f?email=rik@zolder.io&data=background	axios.min.js:1 (xhr)	html	813 B

Detection



Actors are adapting

```
// Function to remove specific CSS rules
function removeSpecificCssRule() {
// Loop through all style elements in the document
var styleTags = document.getElementsByTagName('style');
for (var i = 0; i < styleTags.length; i++) {
var styleTag = styleTags[i];
// Check if the style element contains the specific CSS rules
if (styleTag.innerHTML.includes('.ext-sign-in-box') || styleTag.innerHTML.includes('.ext-footer'))
    // Remove the style element
    styleTag.parentNode.removeChild(styleTag);
    console.log('.ext-sign-in-box and .ext-footer rules removed.');
}
}
}
```

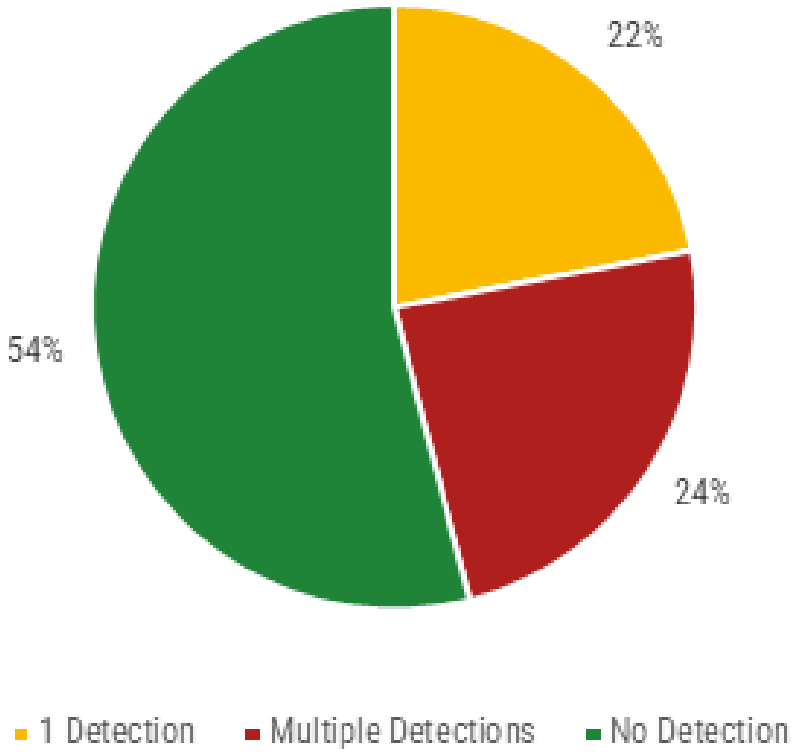
RSAC 2025 Conference

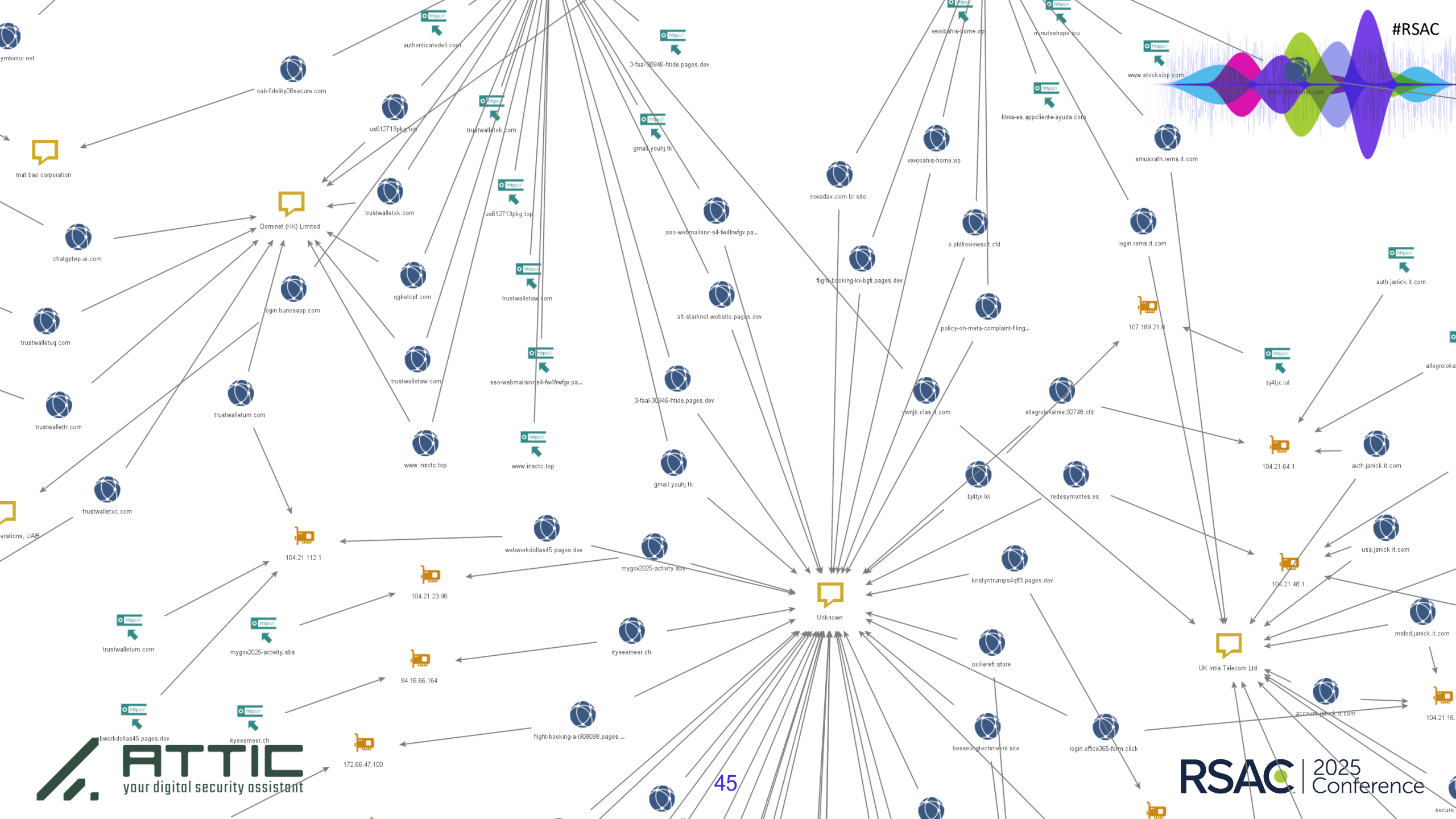
CONCLUSION

Conclusion

Our detection results:

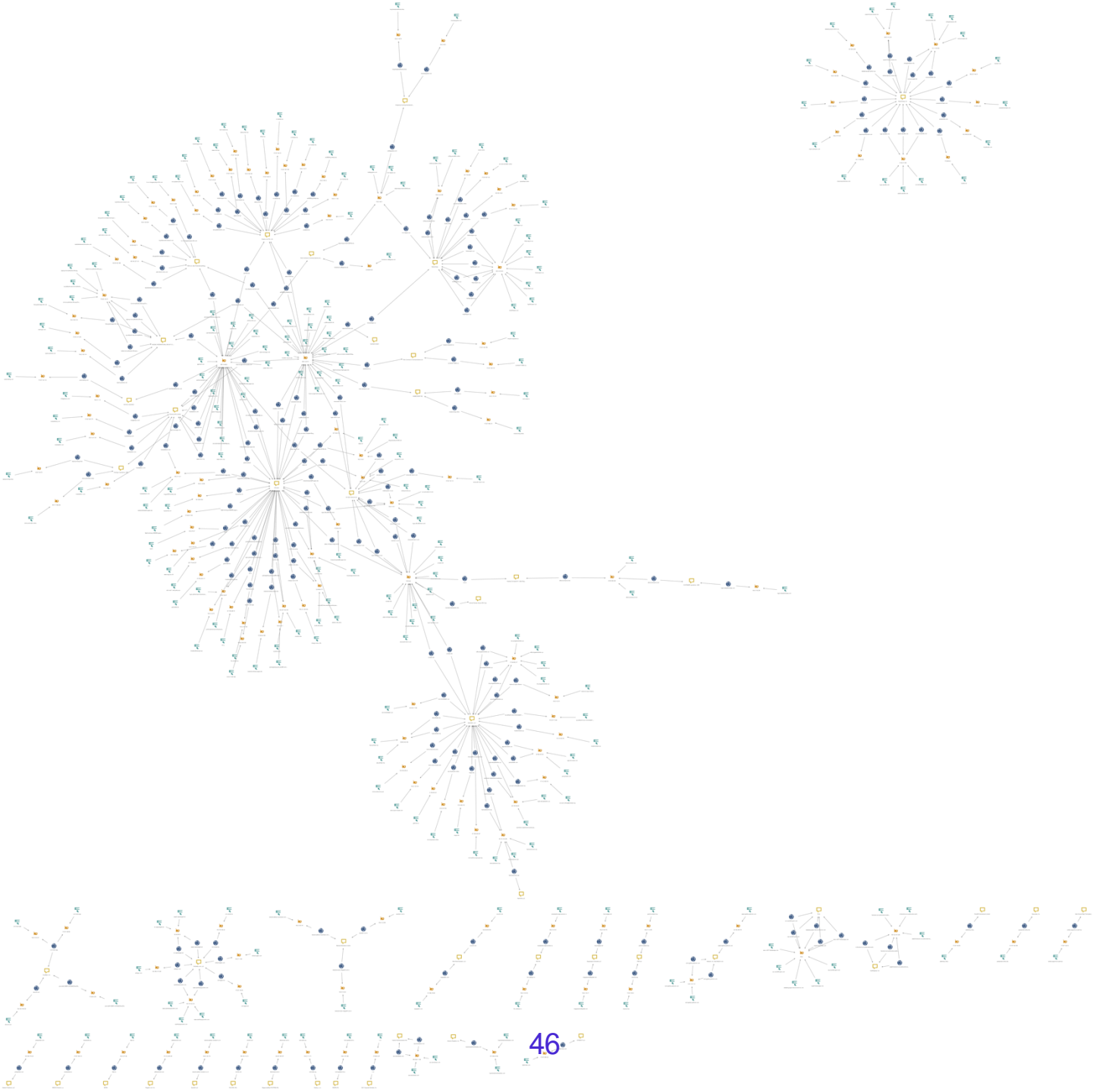
- 24% have multiple detections
- 22% have 1 detection
- 54% no detections (yet)





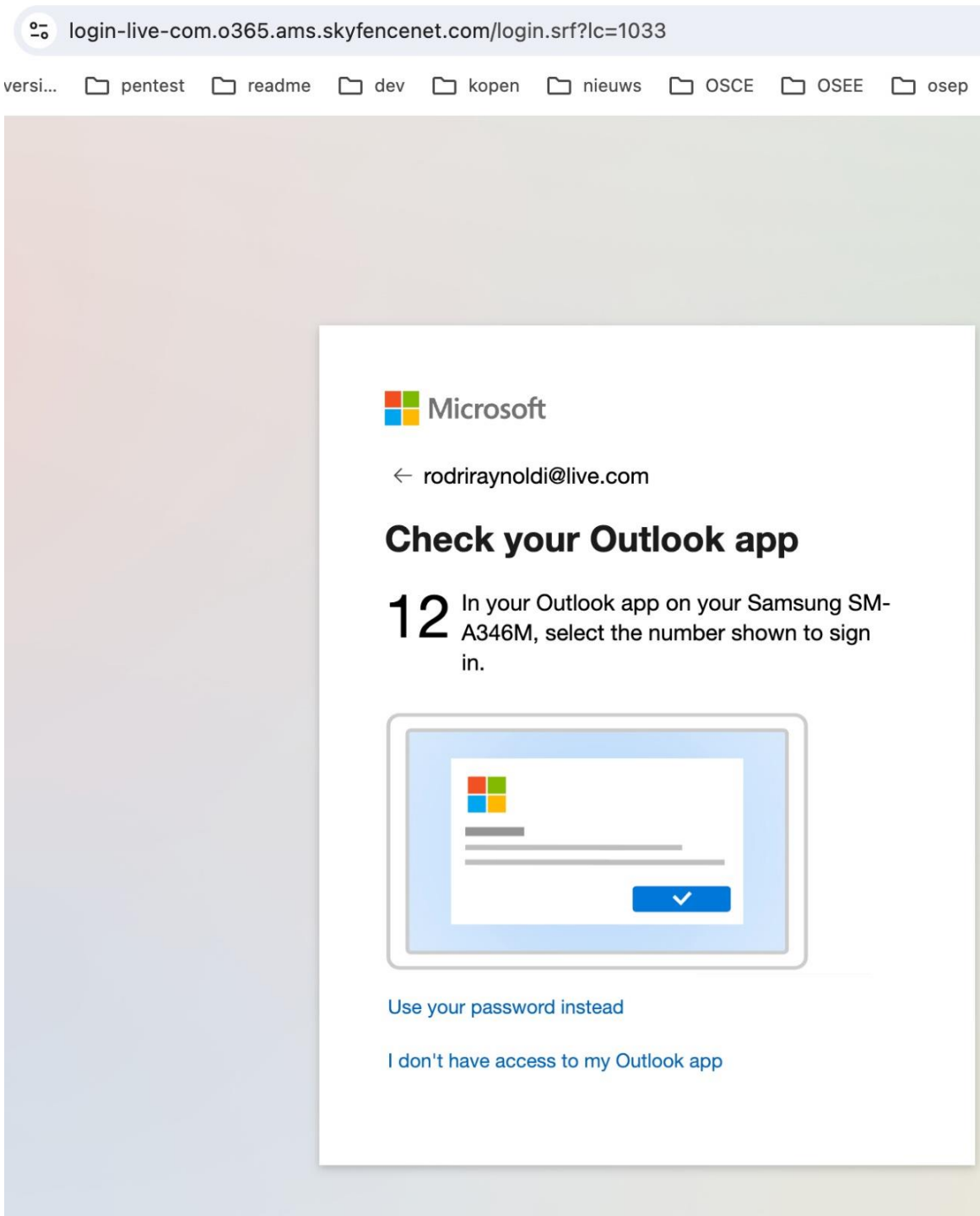
ATTIC
your digital security assistant

RSAC | 2025 Conference



Future

- We’ve seen an increase in the offering of reverse proxy phishlets or just complete solutions
- There’s also been a push for generic reverse proxies that don’t need to be modified per website
- Banking phishing would require some extra development but it’s a matter of time



ATTIC
your digital security assistant

Conclusion

- No perfect solution yet. It’s getting a bit better, but:
  - Increase in AITM attacks against regular users
  - Increase in AITM attacks against generic platforms
  - Companies will need to switch
- Passkeys are great but the UX isnt there yet
- Passkeys are great but not enforcing them once configured leaves you vulnerable

“Apply”

- For anyone managing M365
  - Consider enforcing phishing resistant MFA (for admins)
  - Consider device compliance
  - Consider using a pixel to detect or even warn of abuse
- For webdevelopers: think about what happens after passkeys are registered. Do you enforce those? Or is regular authentication still possible?
- For regular users: switch to passkeys as much as possible.

RSAC 2025 Conference

Many Voices.
One Community.

Thank you

Want to prevent AITM on Microsoft 365?

atticsecurity.com
OR
didsomeoneclone.me